AFOSR project "Quantum Communication Systems"

University of Oxford and UMK Torun

Final Report
15 March 2008

Summary
This document summarises the outcomes of the above project. Achievements include the preparation of the purest photons to date using parametric downconversion, their temporal characterization by interference with a local oscillator and the theoretical study of their propagation in lossy quantum channels. Also, their information capacity due to their continuous mode structure, and the application of this to a secure quantum communications system has been analysed. These photons have been used to generate the first heralded multiphoton entangled states, and the sources have been extended to the multiphoton regime. Also, for the first time a complete detection scheme has been analyzed in terms of a tomographic characterization of its POVMs.

The work completed is summarized as follows:

Work completed and in progress

First 6 months:

- Examples of quantum error-correcting (QEC) codes for photon loss (UMK)
- Analysis of linear manipulations of QEC for photon loss (UMK)
- Conditional operations on QEC codes for photon loss with auxiliary photons (UMK)
- New method for characterizing spectral properties of single photons (UMK)
- Measurement of a density matrix of single photons (UMK)
- Generation of pure-state photons by vacuum engineering (Oxf)
- Analysis of security of qudit communications using continuous degrees of freedom of entangled photon pairs (Oxf)

Second 6 months:

- Analysis of partially correlated depolarizing channels (UMK)
- Analysis of optimal states for precision measurement through lossy channels (UMK/Oxf)
- Entanglement of pure-state photons (Oxf)
- Tomography of photon-number-resolving detectors with local oscillator capability (Oxf)
- Measurement of multiphoton components in parametric down-conversion. (UMK/Oxf)

Summaries of the these follow. (The first section repeats the text of the annual report for completeness. Work accomplished in the second 6-month period is described starting on page 13.)

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
27-03-2008	Final Report	1 August 2006 - 01-Aug-07

4. TITLE AND SUBTITLE Quantum Communications Systems	**5a. CONTRACT NUMBER** FA8655-06-1-3062
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Professor Ian A Walmsley	**5d. PROJECT NUMBER**
	5d. TASK NUMBER
	5e. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) University of Oxford Parks Rd Oxford OX1 3PU United Kingdom	**8. PERFORMING ORGANIZATION REPORT NUMBER** N/A
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) EOARD Unit 4515 BOX 14 APO AE 09421	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) Grant 06-3062

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report results from a contract tasking University of Oxford as follows: The Grantee will investigate.......Photonic quantum sources for scalable Linear Optics Quantum Communications (LOQC). The objective of this workpackage is to develop photonic sources suitable for linear optical quantum communications. This requires the efficient preparation and utilization of single- and multiple photons in pure states, with good modal quality, compatible with guided wave optics

15. SUBJECT TERMS

EOARD, Quantum Communications, Quantum Effects

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18, NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UL	21	JAMES LAWTON Ph. D.
UNCLAS	UNCLAS	UNCLAS			**19b. TELEPHONE NUMBER** *(Include area code)* +44 (0)1895 616187

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39-18

Publications:

1) W. Wasilewski and K. Banaszek, *Protecting an optical qubit against photon loss*, Phys. Rev. A **75**, 042316 (2007)
2) K. Banaszek and W. Wasilewski, *Linear-optics manipulations of photon-loss codes*, Proceedings of NATO Advanced Research Workshop "Quantum Communication and Security"
3) W. Wasilewski, P. Kolenderski, and R. Frankowski, *Spectral density matrix of a single photon measured*, Phys. Rev. Lett. (2007)
4) L. Zhang, Ch. Silberhorn and I. A. Walmsley, *On the security of key distribution using continuous variables of entangled photon pairs*, accepted for Physical Review Letters.
5) P. Mosley, J. Lundeen, Ch. Silberhorn, A. U'Ren and I. A. Walmsley, *Generation of broad-band single photons in pure quantum states*, accepted for Physical Review Letters.

First 6 month period (duplication of annual report).

I. Experimental Production of Pure Single-Photon States

The simultaneous production of single photons from multiple sources represents a significant step towards realistic schemes for quantum information processing (QIP) using linear optics [1]. Several groups are currently working towards this using photon pairs produced in either parametric downconversion (PDC) [2, 3, 4, 5] or four-wave mixing [6], where one photon from each pair is used to herald the presence of the other. Some impressive results have been achieved to date, however, all these sources of photon pairs exhibit strong spectral correlations, resulting in the need to use tight spectral filters to achieve high visibility interference with the heralded single photons. This puts a fundamental limit on the purity of the photons produced for a given count rate [7]. Similar requirements are necessary for QIP with continous-variable states, but with an added sensitivity to the loss that accompanies filtering.

We utilize a technique of spectral engineering of the two-photon states produced from PDC that ensures that these spectral correlations are never created in the first place. This is achieved by group velocity matching the fields in the nonlinear medium, allowing photon pairs to be produced directly in uncorrelated states, rather than generating pairs indiscriminately and discarding any exhibiting correlations. Hence we demonstrate high visibility interference without the need for any spectral filtering.

Producing a heralded photon in a pure state relies upon having an initial twophoton state that is separable in all degrees of freedom. Otherwise, detecting one photon, and therefore tracing over its unresolved degrees of freedom, will leave the heralded photon in a mixed state. As far as the spectral degree of freedom is concerned, the obvious way of achieving this is by using spectral filters, but the purity of the heralded photons produced by this method tends to one only as the filter bandwidth tends to zero [7]. In contrast, by using a broad bandwidth pump and exploiting the flexiblity in the dispersion of birefrigent crystals through type II PDC, we implement a more elegant method based on control of the pairs generated rather than elimination of the undesirable ones.

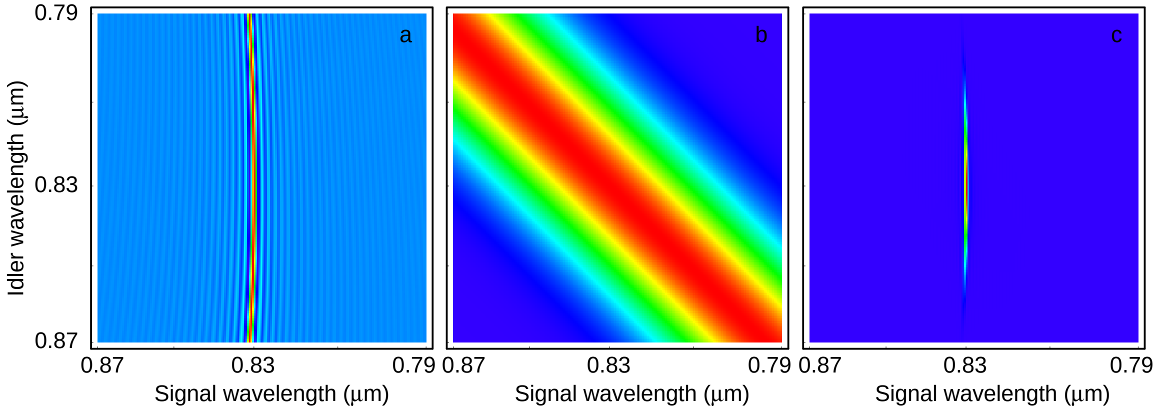

Figure 1: Phasematching function (a), pump fuction (b), and joint spectral intensity for a 20mm KDP crystal pumped at 415nm.

Type II downconversion results in daughter photons that are orthogonally polarized. When travelling through the birefringent nonlinear medium in which the parametric interaction occurs, these photons have different group velocities. By choosing the pump and downconversion frequencies and the nonlinear medium, we can arrange that the group velocity of one daughter photon (in this case the o-ray photon) has the same group velocity as the pump (e-ray). Plotting the phasematching function for this case demonstrates that it is almost completely uncorrelated in frequency ("vertical"), as shown in Fig. 1. When combined with a broadband pump function this results in a two-photon state that is factorable in frequency; it can be written as the product of terms dependent on only the e–ray frequency with terms dependent on only the o–ray frequency. This product state can therefore have one photon traced out with the other remaining in a pure state.

In general, a vertical phasematching function requires group velocity matching of the pump pulse with one – and only one – of the daughter photons. We find the required dispersion and birefrigence in collinear type II PDC in a bulk KDP crystal pumped at 415nm. The o-ray daughter photon travels at the same velocity as the e-ray pump in the crystal and is broadband (20nm FWHM) whereas the e-ray photon walks off temporally from the pump and is narrowband (1nm FWHM for a 20mm long crystal). Modeling this two-photon state shows that it has some interesting features. The separability of the state can be quantified by a number of different measures, among them the spectral Schmidt decomposition. By expressing the state as the weighted sum of product states, it can be shown that, for a 20mm long KDP crystal and a plane wave pump, over 99% of the two-photon state is accounted for by the first Schmidt mode – almost a perfectly separable state. However, experimental considerations do not allow the use of a collimated pump in practice. In order to have photons in well–defined spatial modes, the downconversion must be coupled into single mode fibers, allowing for high–visibility interference and simple delivery of the heralded states to subsequent experiments. For high coupling efficiency we require that the downconversion is preferentially emitted into modes which are easily coupled into single–mode fibers; this means focusing into the nonlinear crystals. This can introduce additional correlations into the two–photon states due to the different phasematching conditions experienced by each incident angle in the pump beam. In addition to this the pump beam, the second harmonic of a titanium:sapphire laser, is spatially chirped as a result of tight focusing into the frequency doubling crystal – the frequency of the output from the doubler is closely correlated with angle. Combined with the focusing conditions in the downconversion crystal, this can also result in frequency correlations. Therefore it is essential to have a well-characterized pump beam, careful choice of focusing conditions, and the correct orientation of the nonlinear crystal to ensure factorability.

Two such KDP downconversion sources have been implemented experimentally for use in a multiple-source interferometry experiment, as shown in Fig. 2. The pump is a frequency-doubled Ti:Sapphire oscillator with a bandwidth of 25nm at 830nm, producing 100mW of 415nm pulses after doubling. The broadband nature of the pump allows the phasematching function of the KDP crystal to dominate the joint spectrum of the photon pairs and provides precise timing information.

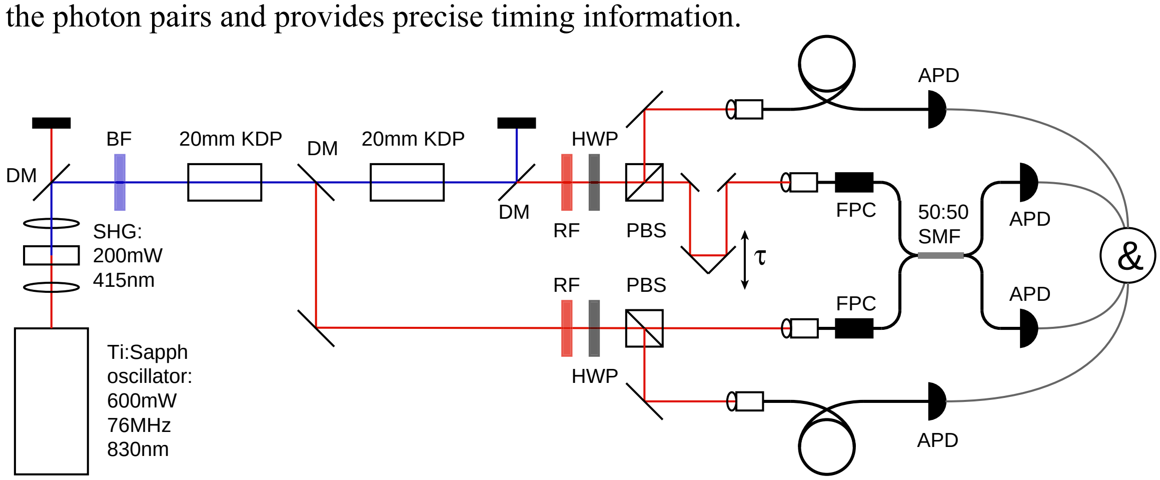

Figure 2: Experimental apparatus.

Photon pairs are generated by the same pulse in each crystal and each pair is split in two at the polarizing beamsplitters. All four photons are coupled into single mode fibers; one photon from each pair is used to herald the other, which is directed into a 50:50 fiber coupler. Using silicon avalanche photodiodes, fourfold coincidences in the two heralding arms and at the two outputs of the 50:50 coupler are monitored as a function of an optical time delay in one input arm. As the time delay is scanned, a Hong-Ou-Mandel type interference is observed in the fourfold coincidence rate, shown in Fig. 3. This visibility will be unity if the photons in the input modes are pure and indistinguishable.
The best experimental result achieved to date is an interference visibility of 94.4 ± 1.6%. This places our source firmly at the forefront of the current experimental state–of–the–art. We have also measured the photon statistics from this source (Fig. 3) using our time-multiplexed photon number resolving detector [8]. These statistics are an alternate measure of the purity, directly relevant to continuous-variable states [4].

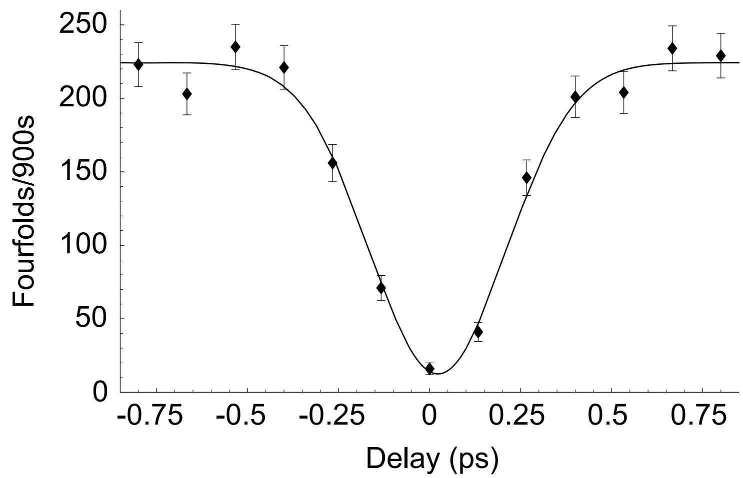

Figure 3: Experimental data. Hong-Ou-Mandel interference dip in fourfold coincidence rate with a visibility of 94.4 ± 1.6%.

Having demonstrated this high–visibility interference at good count rates, we now intend to go on to use the heralded single photons in a variety of novel QIP schemes. The first of these is to demonstrate the first ever heralded NOON state by making a precision phase measurement in a second interferometer. The heralded state will be delivered directly from single–mode fibers following the 50:50 coupler and will therefore already be in a well-defined spatial mode, greatly simplifying any downstream processing.

We have conclusively shown that parametric downconversion in KDP provides a clean method – both conceptually and experimentally – of generating pure, heralded single photons. We are now ready to move forward and employ these photons in new linear optical QIP protocols.

References

[1] E. Knill, R. Laflamme, and G. J. Milburn, Nature 409, 46–52 (2001).
[2] R. Kaltenbaek et al, Experimental interference of single photons, quantph/ 0603048 (2006)
[3] Q. Zhang et al, Experimental Quantum Teleportation of a Two-Qubit Composite System, quant-ph/0609129 (2006)
[4] G. Y. Xiang et al, Demonstration of Temporal Distinguishability in a Four-Photon State and a Six-Photon State, quant-ph/0602015 (2006)
[5] J.-S. Xu, C.-F. Li, G.-C. Guo, quant-ph/0607183 (2006)
[6] J. Fulconis et al, Photonic crystal fibre source of photon pairs for quantum information processing, quant-ph/0611232 (2006)
[7] A. U'Ren, Ph.D. thesis, University of Rochester (2004)
[8] D. Achilles, C. Silberhorn, and I. A. Walmsley, PRL 97, 043602 (2006)

II. Quantum error correction for photon loss

Quantum interference effects are susceptible to uncontrolled interactions with the environment, which can undermine the advantage of quantum-enhanced information technologies. This difficulty was realized very early in the development of quantum information processing, leading to the theory of quantum error correction (QEC). The basic assumption underlying QEC is that errors happen with a sufficiently small probability to apply a perturbative expansion, whose leading orders can be dealt with efficiently by preparing suitable robust states of multiplicated physical systems. Historically, attention was focused first on ensembles of two-level systems – physical qubits – that interact independently with their environments in an arbitrary way. However, in certain implementations the dominant interaction with the environment has a more specific form, enabling one to optimize the QEC strategy.

In the context of quantum communication, we addressed amplitude damping leading to photon loss as a dominant decoherence mechanism in photonic implementations of quantum information technologies. We demonstrated limitations of passive (i.e. not involving auxiliary conditional detection) linear optics networks for this task. Further, we introduced a simple three photon code for encoding one logical qubit that is capable of correcting for the loss of one photon. We derived a complete set of passive single-qubit gates, and demonstrate the possibility to implement both state and process tomography with linear optics and photon counting. This opens up prospects for proof-of-principle demonstrations of the three-photon code using present experimental capabilities. We also presented a conditional encoding circuit that maps an arbitrary state of an input qubit in dual-rail representation onto the encoded subspace. Although its intrinsic success rate is about 5%, we showed that it can be boosted to the near-deterministic level using a suitably chosen teleportation protocol.

A general passive linear optics transformation of a system of N modes can be written as unitary matrix acting on creation (or, equivalently, annihilation) operators of the field modes. The unitarity of the matrix guarantees the preservation of commutation relations for the field operators. Any linear-optics transformation can be reversed, therefore the labels of input and output representations are purely conventional. It turns out that this unitary transformation preserves the recoverability condition for noise operators corresponding to one-photon loss. This means that after the application of the network the code subspace remains a photon-loss code. This property reflects the fact that in our error model the correctability condition is independent of the specific modal decomposition. Indeed, the third party monitoring the leaked field can decompose it in an arbitrary basis of modes and measure them individually for the presence of a photon. Because the damping coefficients are assumed to be identical for all the modes, such a procedure performed on the leaked field does not alter the error model.

The fact that the photon-loss code is preserved by passive linear-optics transformations has important implications for encoding and decoding. Suppose that we start from a qubit in the standard, dual-rail representation, with the aim of mapping it onto the encoded subspace. A simple way to accomplish this would be to combine it with auxiliary modes prepared in a certain state and apply a passive linear optics transformation. However, the reversed version of the argument presented above implies that if the output is a photon-loss code, then the input needs to be such a code as well. This means that the input qubit itself is protected against photon loss, which obviously is not the case for the dual-rail representation. The same applies to decoding: if we know a priori that no photon loss occurred, we cannot convert the encoded qubit back into the dual-rail representation using a passive network. Therefore, there cannot exist a passive network that would work more universally for the input affected by errors and provide a decoded qubit with the error syndrome contained in the state of auxiliary modes.

A slightly more complicated argument can be applied to single-qubit gates operating on encoded qubits implemented with linear optics. If such gates formed a continuous group, one could find a one-parameter subgroup, whose generator would be bilinear in field operators. However, the same generator appears in the recoverability condition, and therefore its action on the code subspace is trivial. This argument shows that the group of single-qubit gates can be at most discrete.

Equipped with these general results, we approached the task of processing a single encoded qubit with linear optics and conditional detection. Starting from the simplest code based on three photons in three modes, we discussed a scenario when the three signal modes carrying the encoded qubit are combined with an arbitrary number of auxiliary vacuum modes and subjected jointly to a unitary linear transformation. The output in the three signal modes is accepted conditionally on the detection of zero photons in all the auxiliary modes. This procedure includes deterministic gates as a specific case. If the auxiliary modes are prepared and detected in the vacuum state, the transformation of the state contained in the signal modes depends only on a 3x3 sector of the entire unitary matrix describing the transformation of the modes. A detailed analysis of the algebraic equations showed that in the encoded space one can implement the rotation group of a tetrahedron.

Finally, we presented a universal linear-optics circuit that converts a single qubit in the standard dual-rail representation into a qubit encoded in the loss-proof basis. As we demonstrated, such a procedure cannot be implemented deterministically using a passive linear-optics network. Our circuit combines the input qubit carried by one photon in a superposition of two modes with four auxiliary single photons, and conditions the output upon the detection of a specific sequence in the three monitored modes. The three remaining output modes that leave the circuit contain then the encoded qubit. The overall success rate of the encoding circuit is equal to 4.86%. We performed a numerical search over networks that combine in an arbitrary way all the six input modes and an arbitrary number of additional vacuum modes, which did not improve the success rate. The presented encoding circuit can be however applied to encode a single copy of a qubit in an unknown state by using it "off-line", following the idea of teleportation-based computational primitives. The first step is to apply the encoding circuit to a qubit that belongs to a maximally entangled pair composed of two photons, repeating the procedure on freshly prepared pairs until the successful operation is achieved. Then the second qubit from the successful pair is measured jointly with the input qubit using a projection onto particularly defined four orthogonal maximally entangled states. The measurement step can be performed nearly deterministically using universal linear-optics quantum circuitry with auxiliary single photons and fast feed-forward. This leaves the encoded qubit in the desired state up to one of the tetrahedron which can be compensated for by an optional application of one of the deterministic linear-optics transformations.

III. Characterization of single-photon wave packets

Development of single photon sources brings the promise of implementing novel quantum-enhanced technologies. In many applications, including quantum computing based on linear optics photon sources are required not only to deliver single light quanta, but also to supply them in a well defined mode. This is a necessary condition for quantum interference between independent sources which is required in the above schemes. Also observation of three and more photon interference effects puts stringent requirements on the sources. Besides, characterizing single photons is also interesting from the fundamental point of view. Historically photons were first described within the framework of quantum field theory, but more recently it was pointed out that a photon wave function can be introduced. This kind of description, generalized by the introduction of the density matrix constructed out of projectors on the states with specific wavefunctions, seems to be the most elegant and effective theoretical tool for developing quantum-enhanced technologies.

Up till now measurements of polarization and spatial density matrix of a single photon were reported. The temporal characteristics of single photons were assessed only by verifying whether they interfere with other sources or between themselves. We proposed and demonstrated a method for complete characterization of the temporal degree of freedom: a measurement of the spectral density matrix of a single photon. We showed that the two-dimensional map of coincidence counts recorded as a function of delays between an unknown photon and a pair of weak reference pulses can be used to reconstruct the magnitude and the phase of the density matrix.

Our method for measuring the density matrix is based on the Hong-Ou-Mandel interference effect between the single photon to be characterized and a local oscillator (LO) pulse of known shape attenuated to a single photon level. The visibility of the two-photon interference dip is proportional to the overlap between the modes of interfering photons. Figuratively speaking, by modulating the local oscillator spectral amplitude and measuring the dip we can examine the single photon wavefunction from many directions. For a suitable class of LO pulses this suffices to retrieve the spectral density matrix of a single photon. In a broad sense, our experiment is a single photon analog of the homodyne method for measuring quantum correlations within a light pulse. Indeed the density matrix describes correlations within a single photon pulse. The first part of the experimental setup is a Michelson interferometer which serves as a LO pulse modulator, preparing a pair of pulses with controlled arrival times. The second part is the beamsplitter on which the Hong-Ou-Mandel interference occurs.

We presented a measurement for a type-I spontaneous down-conversion process in a bulk beta-barium borate (BBO) crystal, and compared the results of the reconstruction with theoretical predictions. Details of the experimental setup are as follows. The master laser (RegA 9000 from Coherent) produces a train of 165 fs FWHM long pulses at a 300kHz repetition rate centered at 774 nm, of which we use 300 mW average power. Most of the energy goes to the second harmonic generator, based on a 1 mm thick BBO crystal cut for type-I process. Ultraviolet pulses produced this way have 1.3nm bandwidth and 30 mW average power. They are filtered out of fundamental using a pair of dichroic mirrors DM and a color glass filter BG (Shott BG39), and imaged using 20cm focal length lens IL on a downcoversion crystal X, where they form a spot measured to be 155 um in diameter. The crystal X is a 1 mm thick BBO crystal cut a 29.7 deg to the optic axis, and oriented for maximum source intensity. A portion of down-converted light propagating at an angle of 2.5 deg to the pump beam passes through a 10nm interference filter centered at 774.5nm and is coupled into a single mode fiber. This defines the spatial mode in which the down-conversion is observed. About 4% of energy of master laser pulses is reflected towards an LO preparation arm. The pulses first go through a half wave plate HWP and a polarizer P allowing for fine control of the energy. Then they are delayed in a computer-controlled delay line. Next the pulses enter a Michelson interferometer in which one mirror moves on a precision computer controlled stage allowing for generation of double pulses with a well-defined temporal separation. Finally the double pulses are attenuated to contain less than 0.1 photon on average and coupled to a single mode fiber, where their polarization is adjusted using a fiber polarization controller FPC to match the polarization of the photon coming from the downconversion source. Both the downconversion and local oscillator photons interfere in a 50/50 singlemode fiber coupler and are detected using single photon counting modules SPCM (PerkinElmer SPCM-AQR-14-FC) connected to fast coincidence counting electronics (suitably programmed Virtex4 protype board ML403 from Xilinx) detecting events in coincidence with master laser pulses.

We compared the reconstructed spectral density matrix of a single photon with theoretical calculations. The theoretical model used in these calculations assumed the exact phase matching function of the nonlinear crystal and the ultraviolet pump pulse shape computed from the measured envelope. The transverse components of the wave vectors for the pump and down-converted beams were treated in the paraxial approximation. The spectral density matrix was calculated for coherent superpositions of plane-wave components of the down-conversion light that add up to localized spatial modes defined by the collecting optics and single-mode fiber. The other photon from the source, which remains undetected, was traced out assuming that it can propagate at any direction and have any frequency that is consistent with the conservation of energy and perpendicular momentum in the downconversion crystal.

IV. Partially correlated depolarizing channel (work in progress)

A fruitful approach to protect quantum systems from decoherence introduced by uncontrolled interactions with the environment is to use symmetries exhibited by those interactions. When elementary quantum systems in an ensemble are coupled to the environment in an identical way, it is possible to identify certain collective degrees of freedom that turn out to be completely decoupled from the interaction, thus preserving quantum coherence. This approach is the basic idea behind decoherence-free subspaces and subsystems (DFSs), which can be implemented in a number of physical scenarios, including polarization of photons transmitted through a birefringent fiber, spins of electrons in an external magnetic field, and communication in the absence of a common reference frame. The existence of DFSs allows one to encode or communicate reliably both classical and quantum information, which has been demonstrated in first proof-of-principle experiments.

The purpose of this work is to go beyond the standard theory of DFSs and to analyze a scenario when the interactions of elementary systems with the environment are not necessarily identical. Specifically, we will consider a sequence of qubits affected by random unitary transformations. In the standard DFSs model all unitaries are the same, enabling one to apply the standard decomposition into multiplicity subspaces based on angular-momentum algebra. In contrast, we assume that correlations between unitaries affecting consecutive qubits are characterized by a probability distribution describing isotropic diffusion on the SU(2) group. Such a distribution has a number of invariant properties that result in the existence of a single real parameter which defines the strength of correlations. This will enable us to investigate the continuous transition between the extreme regimes of perfect correlations and independent transformations of consecutive qubits.

V. Multiphoton components in parametric down-conversion (work in progress)

We constructed a loop detector which enables one to resolve multiphoton events by splitting input pulses into multiple time slots that are monitored separately by avalanche photodiodes. We plan to detect photon statistics of twin beams generated by means of parametric down-conversion. The down-conversion medium will be pumped by doubled pulses from a regenerative amplifier, which provides sufficient energy in a single pulse. Reconstruction will be achieved using maximum-likelihood approach. Our aim will be to observe non-classical features of photocount correlations and analyze their consequences for the security of quantum cryptography.

VI. Photon number resolving detectors (work in progress)

Time multiplexed detectors (TMD) provide an easy way of overcoming the binary nature of Avalanche Photo Diodes (APD). Pulses under investigation are split and delayed in fibre networks and then detected by APDs. We have recently implemented electronic gating systems to reduce noise and a computer controlled data acquisition system to speed up the data acquisition. This allows us to run TMDs at a speed which is determined solely by the repetition frequency of the pulsed signal and the intrinsic time delay of the TMD. This means of characterising quantum states of light in the photon number bases has been used as a single TMD to measure the statistics of a parametric down conversion (PDC) source and run on one of the two beams. For a full characterisation it is necessary to measure the joint photon number statistics of both polarisation components at the same time. This requires the synchronised operation of at least two TMDs. The aim of this project was to synchronously run two TMDs and to extend the mathematical treatment of the TMD, i.e. the convolution and loss matrices, to the case of the joint statistics. Finally a PDC, coupled into single mode fibre, was set up and some joint statistics of different sources of light were taken.

Two different fibre networks and data acquisition units were previously built in the group and as a first step used as single TMD. A major problem in running multiple TMDs is the synchronisation of the data acquisition. The data acquisition programme cannot be triggered simultaneously within the necessary 100ns timeframe. This means that electronic signals from a particular detection event are registered at different time slots in the two input channels of the computer. Since the temporal relation between two events can not be extracted from the data, this ultimately destroys any information on the joint events. This was overcome by controlling the counting via a computer card using a gating pulse synchronized to the drive laser. We were able to synchronize the data acquisition by using the same gate signal for both TMDs.

The time gating used to filter noise from the downconversion modes is highly sensitive to the electronic gate length (about 4ns), and the correct temporal alignment of the trigger and the signal is crucial. Since the downconversion signal which to be measured suffers from a fluorescence background, it is difficult to find the characteristic TMD pattern and align it to the gating. The coincidences due to downconversion are distributed into eight time slots by the TMD network and are thus even weaker. It proved useful to first align a signal without using the TMD fibre network. The additional delay introduced by the TMD fibre network is well known and can be compensated for, to get a rough alignment. We finally fine-tuned the delay with a variable delay box to a optimize the signal. A reference signal strength had been determined before with a coincidence measurement. The concept used for synchronisation could in theory be extended to even more TMDs, only limited by the number of available channels on the computer counter card. With the use of single mode fibres, losses become more critical: coupling efficiencies decrease and losses in the fibre network are higher. The losses can be compensated for in the data analysis, if a value for the efficiency is accurately known. In addition to the direct losses in the fibre network, coupling losses and connector losses must be included, too. We used several ways – based on the concept of a self-referencing detector - to extract this efficiency from the measured data using prior information. Generally, the fibre networks used in the experiment show significantly different optical losses and for both networks the losses seem to be much higher (more than 30%) than expected.

We ran two TMDs synchronised to obtain joint click statistics at data acquisition rates of more than 1 MHz. We took several measurements on a coherent states beam, which was split and fed into two TMDs at variable splitting ratios. The results obtained are consistent with the expected Poissonian statistics. Using PDC sources, only low click numbers could be registered and no significant deviation form Poissonian statistics was established. The calculated efficiencies for the loss treatment vary depending on the calculation method used and are very low. Accounting for losses with these efficiencies gives unphysical negative photon numbers – this might be due to the low efficiencies which are at the boundary of validity of the loss treatment. The second possible reason for this, namely wrong a priori assumption, is rather unlikely, based on previous experiments with this particular PDC source and our own coincidence measurements. A speculative possibility for the a priori information to be wrong is too much fluorescence overlaying the downconversion photons.

Higher photon numbers make the observation of non-Poissonian features easier, which calls for higher pump power and better mode matching of the pump beam, more efficiency and an immense increase in data points. Since higher photon number contributions happen with a low probability the amount of data points taken must increased by several orders of magnitude to get a significant contribution. The expected thermal statistics might also be obscured by the bandwidth of the downconversion signal. Since filtering with interference filters reduces the single counts to dark count level, effort should also be put into increasing the downconversion rate.

VII. Precision measurement through lossy quantum channels (work in progress)

In this project we attempt to exploit entanglement in quantum systems for precision measurements in optical setups, particularly high precision interferometry. The standard purpose of interferometry -the measurement of phase differences of two states- has important applications, for example in the determination of time or frequency standards, in imaging and in communications, and it is thus highly desirable to measure this phase as precisely as possible using the smallest number of resources.

The basic model of an interferometer consists of an input state, an operation which induces a phase on this state and an output state which is measured in order to obtain information about the phase. It has been shown that the accuracy of the estimated phase using classical strategies, i.e. strategies where neither the input state nor the measurement make use of quantum correlations, can be significantly improved by using entanglement. However, most of these works ignore the unavoidable presence of noise in experiments. Highly entangled states are typically more sensitive to noise than non-entangled states, an effect that threatens to decrease or even remove completely the expected gain in precision.

The goal of this project is to find optimal strategies for phase estimation in the presence of noise by using entangled input states of light. To this end we make use of already established inequalities that provide lower bounds on the uncertainty of the estimated phase that depend only on the input state of the interferometer.

In the first step we minimize this lower bound with respect to the input state. We have done this already for a certain class of entangled input states using two modes of the electromagnetic field leading to a state that minimizes the uncertainty of the estimated phase in the presence of photon loss. We furthermore investigate different strategies to operate the interferometer. In particular, given a total number of photons, we could send them all at once through the interferometer or we could send smaller ``packets'' of photons sequentially through the interferometer. The latter strategy promises to improve the precision of the estimated phase even further.

In the second step we will find optimal measurement strategies for readout of the output state of the interferometer. These readout methods will be designed to achieve the previously calculated lower bound (or at least approach it as closely as possible). This will be done either analytically or via numerical optimization methods.

In the future we will apply these steps to different kinds of input states. Due to the large number of degrees of freedom offered by electromagnetic fields there are numerous possibilities, e.g. ``squeezed'' states of light. Furthermore we will extend our research to more than two modes of the electromagnetic field. It has been shown in qubit systems that the accuracy of phase estimation is improved if the number of qubits exceeds two. We will investigate if this is the case if more than two modes are used.

<u>Second 6 month period.</u>

- Analysis of partially correlated depolarizing channels (UMK)
- Analysis of optimal states for precision measurement through lossy channels (UMK/Oxf)
- Entanglement of pure-state photons (Oxf)
- Tomography of photon-number-resolving detectors with local oscillator capability (Oxf)
- Measurement of multiphoton components in parametric down-conversion. (UMK/Oxf)

VIII. Analysis of partially correlated depolarizing channels

When elementary quantum systems in an ensemble are coupled to the environment in an identical way, it is possible to identify certain collective degrees of freedom that turn out to be completely decoupled from the interaction, thus preserving quantum coherence. This approach is the basic idea behind decoherence-free subspaces and subsystems (DFSs). In our effort, we went beyond the standard theory of DFSs and analyzed a scenario when the interactions of elementary systems with the environment are not necessarily identical. Specifically, we considered a sequence of qubits affected by random unitary transformations. In the standard DFS model all unitaries are the same, enabling one to apply the standard decomposition into multiplicity subspaces based on angular momentum algebra. In contrast, we assumed that correlations between unitaries affecting consecutive qubits are characterized by a probability distribution describing isotropic diffusion on the SU(2) group. Such a distribution has a number of invariant properties that result in the existence of a single real parameter which defines the strength of correlations. This enabled us to investigate the continuous transition between the extreme regimes of perfect correlations and independent transformations of consecutive qubits. The obtained results can be applied to different physical systems used for quantum communication-e.g., spins traveling in a fluctuating external magnetic field and photons traveling in a fiber with randomly varying birefringence. The model generalized the standard DFS theory when the time separation between qubits sent through the channel is not negligible in comparison with the characteristic time of environment fluctuations. One can easily imagine such a situation in the case of spins traveling relatively slowly in a randomly varying magnetic field or photons traveling down a fiber in the extreme regime when large temporal separations between photons need to be introduced or sequences of photons are long enough to reach the time scale of birefringence fluctuations.

We derived general expressions for the action of the channel using the angular momentum operator algebra that use only finite summations and standard quantities used in the theory of angular momentum. These general formulas were specialized to the case of three qubits, which turned out to have a number of interesting properties. We maximized the classical capacity of the three-qubit channel, and presented the optimal ensemble of states attaining it. Rather surprisingly, for imperfect correlations the optimal ensemble needs to be based on *nonorthogonal* states. Although the fact that the use of nonorthogonal states may be necessary for optimal classical communication has been known, such channels rarely appear in physically motivated scenarios.

We compared the optimal capacity with the one that can be achieved when one is restricted to the use of orthogonal states and indicated orthogonal states that perform almost optimally. We also calculated and analyzed the optimal coherent information, which provided certain information about the quantum capacity of the channel. This provides a full description of the properties of the three-qubit channel and allows one to address quantitatively effects of deviations from the assumption of perfect correlations.

IX. Analysis of optimal states for precision measurement through lossy channels

Exploiting non-classical, entangled states of light for optical interferometry promises to improve the precision of phase estimation significantly. In an optical interferometer incident light is sent through a reference path and a sensor path. A change in the effective refractive index in the sensor path, e.g. induced by a sample, results in a phase shift which is then attempted to be measured as precisely as possible. Numerous, important applications like the determination of time and frequency standards, optical imaging and microscopy would greatly benefit from a gain in precision in the estimated phase beyond the classical shot noise limit. It has been shown that certain classes of highly entangled states of light ideally increases the measurement accuracy by a factor which is proportional to the square root of the employed resources -the energy required for the experiment- leading to Heisenberg limited interferometry, the ultimate bound in accuracy. However, most of the work done in this field so far ignores the unavoidable presence of noise in experiments. Highly entangled states are typically more sensitive to noise than non entangled states, an effect which threatens to decrease or even destroy completely the expected gain in precision.

We addressed this problem by analyzing the behavior of these states under the influence of photon loss, which is the typical source of noise in an optical interferometer, and studied how this affects the accuracy of phase estimation. We showed that for loss rates which are typically expected in experiments, states which would lead in the absence of noise to Heisenberg limited phase estimation are indeed so fragile that their use would have no advantage in practice. We therefore studied alternative states and strategies which are more robust with respect to noise and showed that the accuracy of phase estimation can be improved beyond the classical shot noise limit. To this end we analyzed two scenarios:

In one setup it is assumed that photon losses are induced by the sample in the sensor path of the interferometer leading to losses in one channel of the interferometer. In this case we showed that we can effectively optimize the input state such that the classical shot noise limit can be greatly exceeded. In fact, under the realistic assumption 10-15% losses the accuracy can be improved by a power of ~1.6 (which has to be compared to the maximum gain of a power of 2.0 corresponding to the Heisenberg limit). We showed that this improvement is the best possible for input states with a definite photon number and photon loss in one channel. A drawback of the optimized states is that they can have a complicated structure and therefore are difficult to prepare in an experiment. We showed that optimized two-component states, i.e. states which have a much simpler structure, lead to almost the identical accuracy for loss rates smaller than about 25%. This is important since two-component states might be easier to generate experimentally than the more complex optimal states.

In another setup we assumed the presence of noise in both channels of the interferometer. Here we analyzed particular classes of robust input states which lead to an improvement in precision compared to the classical shot noise limit. The gain in precision is not as high as in the first setup, however, this is expected since the second scenario allows for more photon loss events.

For both scenarios we furthermore developed different strategies to operate the interferometer. In particular, given a total number of photons, we could send them all at once through the interferometer or we could send smaller ``packets" of photons sequentially through the interferometer. The latter strategy does not improve the scaling of the accuracy with the employed resources. Nevertheless we showed that it improves the absolute precision of the estimated phase compared to the shot noise limit by, e.g., factors of about 1.3 and 1.7 for the two scenarios and a loss rate of 10%.

One of the important results of our work is that highly entangled states from which it was assumed that they lead to a maximally gain in accuracy for the purpose of phase estimation are not useful in the presence of photon loss. We therefore systematically examined alternative states which are more robust and lead in the presence of noise to a better gain than highly entangled states. Our work can therefore help to improve the design of high precision interferometers.

X. Entanglement of pure-state photons

Measurement of physical quantities is central to all sciences, and improvements in the precision have lead to not only more detailed knowledge, but also new fundamental understanding. A crucial question is with what precision such measurements can be made. It turns out that the laws of quantum theory put lower bounds on the precision that can be achieved in an experiment [1-8].

Optical phase measurements are used in many scientific fields to determine distances smaller than the wavelength of light. The ultimate precision of a phase measurement is governed by the Heisenberg uncertainty principle. It is known that in some cases quantum states of light can be used to increase the precision of phase measurements. The so-called NOON states of light, in which two modes (a and b) of the electromagnetic field are in a superposition of having N photons in mode a and 0 in mode b and 0 photons in mode a and N photons in mode b.

To generate heralded two-photon NOON states, we rely on the local photon-bunching effect of two heralded single photons at a beam splitter, as sketched in Fig. 1. Two spontaneous parametric down conversion (SPDC) sources are simultaneously pumped with broadband pulses (centered at 415nm wavelength) to create two photon pairs (centered at 830nm). One photon from each pair is directed to a different photon-counting detector (triggers 1 and 2). Successful detection of two trigger photons heralds the creation of two sibling photons. Note that there are no spectral filters used in this experiment, which significantly increases the generation rate, and often the heralding efficiency. Spectral filters are often necessary to eliminate the frequency-time correlations that arise in the SPDC process. However, by careful choice of phase matching conditions, one can eliminate such correlations [9]. The heralded single photons are sent to separate input ports of a 50:50 beam splitter (BS1). The photons bunch at the beam splitter, exiting together from either output port of the beam splitter with equal probability, creating the two-photon NOON state heralded by two trigger events.

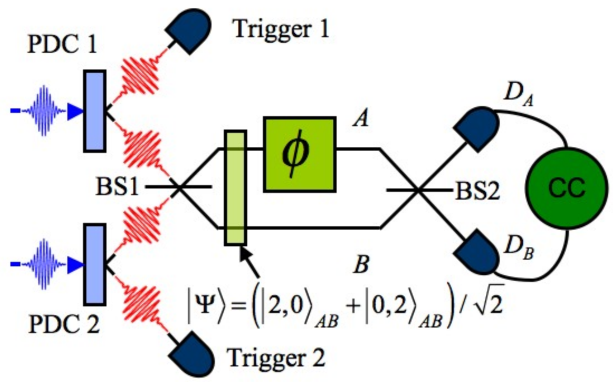

Fig. 1. Experimental setup. A pair of down-conversion sources are simultaneously pumped (PDC1 and PDC2), creating well-timed photon pairs. One photon from each pair heralds the creation of its sibling photon (Triggers 1 and 2). The heralded photons bunch at a 50:50 beam splitter (BS1), resulting in a heralded two-photon NOON state, which then propagates through the two arms of a Mach-Zehnder interferometer with relative phase ϕ between the arms. The two paths recombine on a 50:50 beam splitter (BS2), whose outputs are directed to a pair of photon counting detectors (D_a, D_b), whose coincidence count rate is monitored, contingent upon both triggers firing.

To verify that this is indeed a two-photon NOON state, the output paths of the beam splitter are recombined on another 50:50 beam splitter (BS2), and the four-fold coincidence count rate is recorded as a function of the relative phase, ϕ, between the two paths. Figure 2 shows our experimental data. Note the four-fold count rate oscillates at twice the phase as the two-fold rates, corresponding to the super-resolved phase pattern Eq. (2), while the singles counts (not shown) are constant, implying a non-classical state. The fringe visibility is related to the purity of the photons, and mode overlap of their states. The observed 63% visibility is a lower bound for the purity of the heralded photons produced.

We have demonstrated the generation of a heralded two-photon NOON state from separable, pure single-photon states with a high heralding efficiency, as opposed to previous methods dependent on entangled resources [10]. A visibility of 95% should be possible [9] with more careful alignment of the spatial and temporal modes in the interferometer. With this increased visibility, we plan to implement an iterative-feedback phase-estimation algorithm similar to that recently demonstrated with single photons [11]. The purity and high brightness of this heralded source make it ideal for precision phase measurement.

[1] V. Giovannetti, S. Lloyd, and L. Maccone, “Quantum metrology,” Phys. Rev. Lett. **96**, 010401 (2006).

[2] C. M. Caves, "Quantum-mechanical noise in an interferometer," Phys. Rev. D **23**, 1693-1708 (1981).

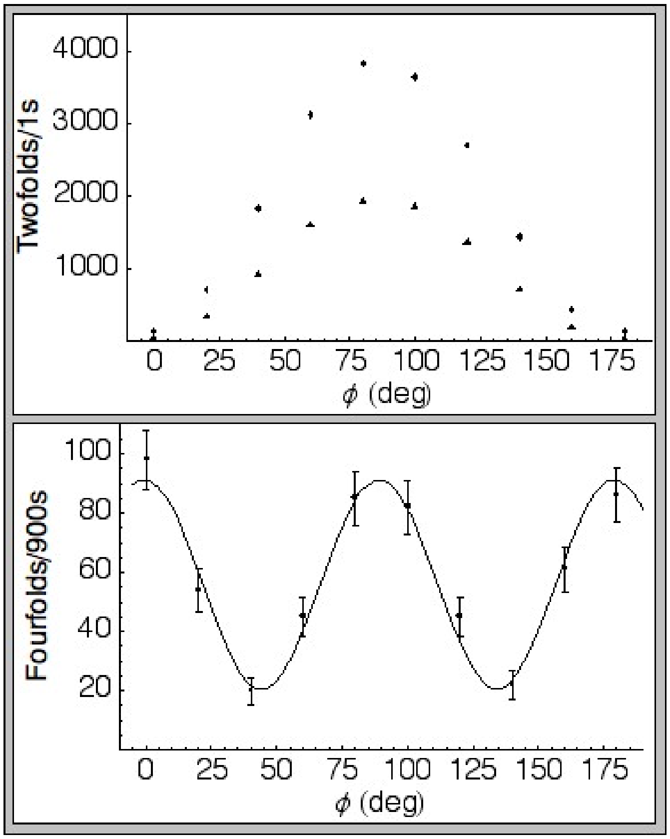

Fig. 2. Experimental results. Two-fold coincidence count rates (top) between detectors D_a(D_b) and D_1 (D_2) (upper (lower) data points) and four-fold coincidences in 900 seconds (bottom) as a function of the relative phase ϕ.

XI. Tomography of photon-number-resolving detectors with local oscillator capability

A quantum protocol or experiment can be divided into three stages: preparation, processing, and measurement. Quantum state tomography [1-3] and process tomography [4,5] respectively prescribe a procedure to completely characterize the first two stages, and have been successfully demonstrated experimentally. State tomography has played a crucial role in identifying and visualizing novel quantum states [6,7]. Process tomography is critical for verifying the operation of quantum logic gates [8] and characterizing decoherence processes [9]. Completing this triad, detector tomography is a procedure for determining the POVM (positive operator-valued measure) set of an arbitrary quantum detector [10]. The POVM contains a matrix for each detector outcome that describes its general action. Thus, without any knowledge of the inner workings of the detector we can predict its response to any input. To the best of our knowledge, detector tomography has not been demonstrated. Here, we report the development of a testbed capable of performing detector tomography on measurement devices acting in the photon-number Hilbert space.

Precise knowledge of the detection POVM set is beneficial for measurement driven quantum information processing, such as cluster-state computing [11]. It is also critical for state and process tomography, which use the measurement as a reference. Recently, it has also been shown that one can perform enhanced measurements by projecting onto non-classical states with a detector [12,13]. Without any need for a theoretical model of the detector, detector tomography can establish which states the detector projects onto, possibly establishing whether they are indeed non-classical. More generally, national standards institutes have used calibrated detectors as a means to distribute standards to industry and science in order to develop new devices. This work enables us to extend this calibration to quantum detectors, which may form basis for potentially disruptive measurement technologies.

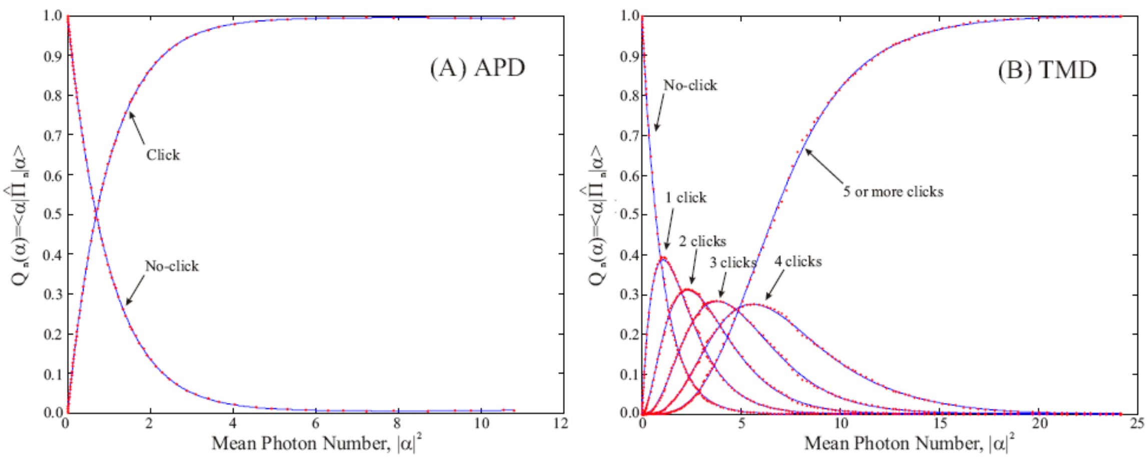

Figure 1. Detector response in terms of the Q-function versus mean number of incident photons for the (A) APD and (B) TMD.

With detection tomography we experimentally characterise a single-photon counter avalanche photo diode (APD, Perkin-Elmer avalanche photo diode: SPCM-AQR-13-FC) and a photon-number resolving detector based on time multiplexing (TMD).

Detector tomography requires a set of reference states ρ that span the space of the POVM set. An identically prepared ensemble of each state is sent to the detector and the frequency P(β) of each detection result β is recorded. Both the APD and TMD measure in the photon number basis and thus, we use weak coherent states as our reference set. The resulting measurement outcome frequencies are equal to the Q-functions (an alternative to the matrix representation) of the POVM elements up to a normalisation constant, as plotted in Figure 1.

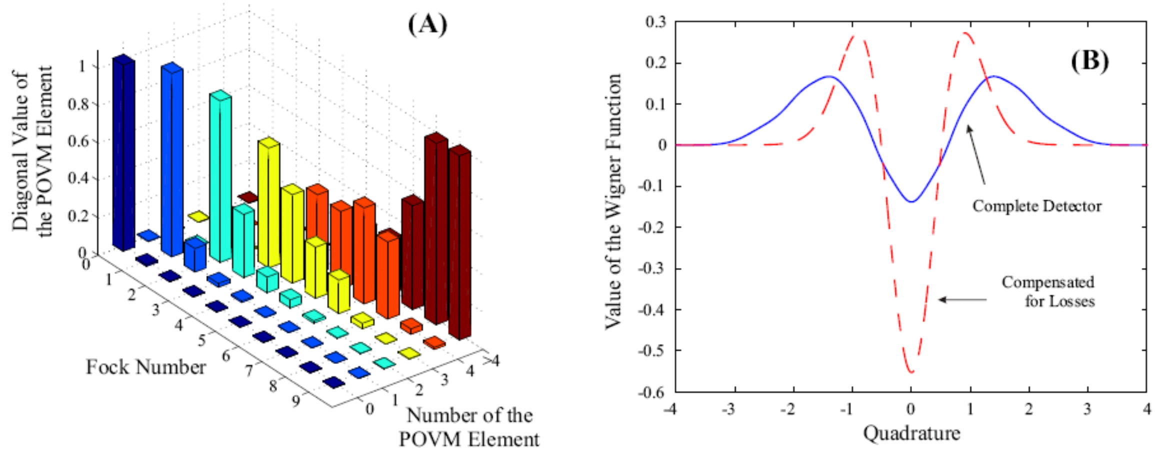

Figure 2. (A) Diagonal values of the reconstructed POVM elements for the TMD with and without losses and (B) Wigner function of the 1-click POVM element of the TMD.

The POVM matrices for the TMD are inferred from the measured data using a semi-definite program. In Figure 2.(A) we show the diagonal values of the TMD-POVM matrices for n=0 up to n>4 clicks. These agree well with theoretical models of the detectors. Next, in order to determine the classicality of the detectors we calculated the Wigner functions of the POVM matrices. In Figure 2 (B), we plot a cross section of the rotationally symmetric Wigner function of the one-click outcome, which becomes negative values at the centre indicating non-classicality.

Quantum detector tomography is the missing element in fully characterising a quantum experiment. We have performed detector tomography on two different detectors and compared the results with models of each detector. The results are in good agreement with theoretical models of the detectors, and thus demonstrate the use of the tomography techniques in detector characterisation.

[1] Smithey, D.T.; Beck, M.; Raymer, M.G.; et al. Measurement of the Wigner distribution and the density matrix of a lght mode using optical homodyne tomography: Application to squeezed states and the vacuum. Phys. Rev. Lett. 1993, 70, 1244.

[2] Dunn, T.J.; Walmsley, I.A.; Mukamel, S. Experimental Determination of the Quantum-Mechanical State of a Molecular Vibrational Mode Using Fluorescence Tomography. PRL 1995, 74, 884–887.

[3] White, A.G.; James, D.F.V.; Eberhard, P.H.; et al. Nonmaximally Entangled States: Production, Characterization, and Utilization. PRL 1999, 83, 3103–3107.

[4] Childs, A.M.; Chuang, I.L.; Leung, D.W. Realization of quantum process tomography in NMR. PRA 2001, 64, 012314.

[5] Mitchell, M.W.; Ellenor, C.W.; Schneider, S.; et al. Diagnosis, Prescription, and Prognosis of a Bell- State Filter by Quantum Process Tomography. PRL 2003, 91, 120402.

[6] White, A.G.; James, D.F.V.; Munro, W.J.; et al. Exploring Hilbert space: Accurate characterization of quantum information. Physical Review A 2001, 65 (1) (Dec), 012301.

[7] Lvovsky, A.I.; Hansen, H.; Aichele T. Benson, O.; J., M.; et al. Quantum State Reconstruction of the Single-Photon Fock State. Phys. Rev. Lett. 2001, 87, 050402.

[8] O'Brien, J.L.; Pryde, G.J.; Gilchrist, A.; James, D.F.V.; Langford, N.K.; Ralph, T.C.; et al. Quantum Process Tomography of a Controlled-NOT Gate. Physical Review Letters 2004, 93 (8) (Aug), 080502.

[9] Myrskog, S.H.; Fox, J.K.; Mitchell, M.W.; et al. Quantum process tomography on vibrational states of atoms in an optical lattice. Physical Review A (Atomic, Molecular, and Optical Physics) 2005, 72 (1), 013615.

[10] Luis, A.; S´anchez-Soto, L.L. Complete Characterization of Arbitrary Quantum Measurement Processes. Phys. Rev. Lett. 1999, 83 (18) (Nov), 3573–3576.

[11] Raussendorf, R.; Briegel, H.J. A One-Way Quantum Computer. PRL 2001, 86, 5188–5191.

[12] Resch, K.J.; Pregnell, K.L.; Prevedel, R.; Gilchrist, A.; Pryde, G.J.; O'Brien, J.L.; et al. Time-Reversal and Super-Resolving Phase Measurements. Physical Review Letters 2007, 98 (22), 223601.

[13] Resch, K.J.; Puvanathasan, P.; Lundeen, J.S.; Mitchell, M.W.; et al. Classical dispersion-cancellation interferometry. Optics Express 2007, 15 (14), 8797–8804.

XII. Measurement of multiphoton components in parametric down-conversion.

The photon statistics of a quantum state of light are an important indication of its character, from which a number of useful measurements of non-classicality may be inferred. Further, in some applications, such as quantum key distribution, the statistics are themselves intrinsically important for determining the security of the communication. We have now made the first, to our knowledge, direct detection of the complete higher order photon number correlations and statistics between two light beams that are completely correlated in photon number (a twin-beam), using a photo-number-resolving detector whose performance is compromised neither by dark-count noise nor by detector inefficiencies. We therefore detect strict photon number correlations for all observed photon numbers including the vacuum. We are also able to identify features caused by the multimode character of the twin-beam source used. A paper has been submitted on this work to Phys. Rev.